НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
КАФЕДРА МАТЕМАТИЧНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ

«На правах рукопису»
УДК 681.3.06:003.26:004.056.5

«До захисту допущено»
В.о. завідувача кафедрою
_____ М.М.Савчук
(підпис) (ініціали, прізвище)
“___” _____ 2020р.

Магістерська дисертація

на здобуття ступеня магістра

зі спеціальності 113 «Прикладна математика»
(код і назва)

на тему: Дослідження сучасних блокчейн-технологій на надійність, доступність та стійкість до розгалудження

Виконав (-ла): студент (-ка) _6___ курсу, групи __ФІ-83_____
(шифр групи)

Горняк Ксенія Станіславівна _ _____
(прізвище, ім’я, по батькові) (підпис)

Керівник професор, д.т.н., с.н.с. Кудін А.М. _____ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант _____ _____ _____
(назва розділу) (науковий ступінь, вчене звання, , прізвище, ініціали) (підпис)

Рецензент _____ _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2020 року

Національний технічний університет України
«Київський політехнічний інститут
імені Ігоря Сікорського»
Фізико-технічний інститут
Кафедра математичних методів захисту інформації

Рівень вищої освіти: другий (магістерський) за освітньо–професійною програмою

Спеціальність: 113 «Прикладна математика»

ЗАТВЕРДЖУЮ
В.о. завідувача кафедрою
_____ М.М.Савчук
(підпис) (ініціали, прізвище)
«___»_____20_ р.

ЗАВДАННЯ
на магістерську дисертацію студенту
Горняк Ксенія Станіславівна
(прізвище, ім'я, по батькові)

1. Тема дисертації Дослідження сучасних блокчейн-технологій на надійність, доступність та стійкість до розгалудження _____
_____
_____ ,
науковий керівник дисертації професор, д.т.н., с.н.с. Кудін А.М. _____ ,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом по університету від _____р. № _____

2. Термін подання студентом дисертації _____

3. Об'єкт дослідження _____
_____

4. Предмет дослідження (Вхідні дані – для магістерської дисертації за освітньо–професійною програмою)
_____
_____
_____

5. Перелік завдань, які потрібно розробити _____
_____
_____
_____
_____

_____

6. Орієнтовний перелік ілюстративного матеріалу _____

_____

_____

7. Орієнтовний перелік публікацій _____

_____

_____

8. Консультанти розділів дисертації*

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

9. Дата видачі завдання _____

Календарний план

№ з/п	Назва етапів виконання магістерської дисертації	Термін виконання етапів магістерської дисертації	Примітка

Студент _____ _____
(підпис) (ініціали, прізвище)

Науковий керівник дисертації _____ _____
(підпис) (ініціали, прізвище)

* Консультантом не може бути зазначено наукового керівника магістерської дисертації.

РЕФЕРАТ

Кваліфікаційна робота містить: 40 стор., 2 рисунка, 14 джерел.

Метою даної роботи є отримання оцінок ефективності та надійності блокчейн-технології у сенсі CAP теореми.

Об'єктом дослідження є протоколи консенсусу блокчейну Casper FFG та Proof of Work.

Предметом дослідження є надійність, доступність та стійкість до розгалудження блокчейну.

Результатами роботи є наведені ідеї для подальшого дослідження надійності протоколу Casper FFG на етапі експлуатації та дослідження невізантійських протоколів консенсуса на властивості CAP теореми.

Результати роботи можуть бути використані для подальшого аналізу систем розподілених обчислень та алгоритмів консенсусу.

Була публікація у журналі «Theoretical and Applied Cybersecurity», Серія КВ № 23760-13600Р d/d Лютий 14, 2019.

БЛОКЧЕЙН, АЛГОРИТМ КОНСЕНСУСУ, CAP ТЕОРЕМА

ABSTRACT

The qualifying work contains: 40 pages, 2 figures, 14 literature references.

The purpose of this work is getting efficiency and reliability evaluations of blockchain technology.

The object of the research are blockchain consensus protocols, Casper The Friendly Finality Gadget, Proof of Work.

The subject of the research is reliability, availability and patition resistance of blockchain.

The results of the work are given assunptiobs and ideas about future researching reliability of Casper FFG consensus protocol and researching non byzantine consensus algorithms in terms of CAP theorem.

The results of the work can be used for the further analysis of the distributed computing systems and consensus algorithms.

There was a publication in the «Theoretical and Applied Cybersecurity» journal, Series KB № 23760-13600P d/d February 14, 2019.

BLOCKCHAIN, CONSENSUS ALGORITHM, CAP THEOREM

ЗМІСТ

ВСТУП

Актуальність дослідження. Ключовими факторами, що характеризують роботу усіх розподілених систем в залежності від їх призначення, є властивості доступності, узгодженості даних та стійкості мережі до розподілення. Надійність блокчейна передусім позв'язана з тим, які з цих властивостей відповідають йому та в якій степіні. Надійність у сенсі розподілених систем зазвичай залежить від кількості чесних учасників протоколу, де чесність визначається надійністю програмного забезпечення вузла.

Метою дослідження Метою дослідження є отримання оцінок оцінок ефективності та надійності блокчейну у сенсі CAP теореми для алгоритмів консенсуса Proof of Work та Casper FFG. Для досягнення поставленої мети необхідно виконати наступні завдання:

1) провести огляд літератури щодо алгоритмів консенсуса;

2) дослідити оцінки надійності протоколів на етапі експлуатації;

3) оцінити надійність поведінки блокчейна при різних варіаціях CAP теореми;

Об'єктом дослідження є протоколи консенсусу блокчейну Casper FFG та Proof of Work.

Предметом дослідження є надійність, доступність та стійкість блокчейну до розгалудження.

Методи дослідження. При розв'язанні поставлених завдань використовувались такі *методи дослідження*: методи теорії імовірностей, методи математичного моделювання.

Наукова новизна отриманих результатів полягає в новому погляді на надійність протоколу Ethereum Casper FFG та порівняння його з робочим Proof of Work.

Практичне значення. Результати роботи можна використати при подальшому аналізі протоколу Casper The Friendly Finality Gadget на

надійність та ефективність у використанні у криптовалюті Ethereum. Результати розгляду блокчейну через призму CAP теореми можна використати для дослідження швидкостей блокчейну при розділенні.

1 ОГЛЯДОВА ЧАСТИНА

В цьому розділі будуть надані відомості про протоколи консенсуса блокчейна, надійність та доступність яких буде досліджуватися — Proof of Work та Casper The Friendly Finality Gadget.

1.1 Біткоін та Proof of Work

Протокол біткоіну повинен досягати консенсусу стикаючись з двома типами перешкод: недосконаліть мережі, така як затримка зв'язку і перебій у роботі вузлів, а також спроба саботувати процес з боку окремих вузлів [1].

Один із конкретних наслідків високої затримки - відсутність уявлення про глобальний часу. Це означає, що не всі вузли можуть досягти згоди з питання послідовності подій, виходячи з спостереження за тимчасовими мітками. Таким чином протокол консенсусу не може містити інструкцію в формі: «Вузел, який відправляє перше повідомлення в кроці 1 повинен зробити X в кроці 2». Це просто не буде працювати, тому що не всі вузли будуть згодні з тим, яке повідомлення було відправлено першим в кроці 1 протоколу [1].

На відміну від традиційної моделі у біткоіну вводиться ідею мотивації майнерів, яка є новою для протоколу розподіленого консенсусу. Мета такого механізму — змусити учасників протоколу працювати чесно. Таким чином біткоін не зовсім вирішує проблеми методу розподіленого консенсусу в цілому, однак вирішує їх зокрема в контексті валютної системи.

Біткоін включає в себе поняття випадковості, алгоритм консенсусу в біткоіні багато в чому покладається на рандомізацію. Крім того йому

вдалося покінчити з поняттям конкретним відправним і кінцевим пунктом консенсусу. Замість цього консенсус відбувається протягом довгого періоду часу, приблизно протягом години в практичній реалізації системи. Але тим не менше по закінченню цього часу, вузли не можуть бути впевнені, що конкретна транзакція або блок були поміщені в реєстр. Замість цього протягом часу ми можемо бачити, що консенсус по блоку буде рости.

Таким чином ймовірність того, що думки щодо транзакції або блоку будуть розходитися, протягом часу буде зменшуватися. Ці відмінності в моделі є ключем до того, як біткоін обходить традиційні результати неможливості для розподілених протоколів консенсусу.

Інша причина в тому, що анонімність - це підкреслене перевагу біткоіна, навіть якщо було б можливо встановити особи всіх вузлів або учасників системи, не обов'язково захочемо це зробити. Хоча біткоін і не гарантує абсолютної анонімності, наприклад тому, що різні транзакції зроблені однією людиною часто можуть бути пов'язані, він як і раніше має властивість, що ніхто не буде зобов'язаний розкривати свою реальну особистість, наприклад ім'я або IP-адресу, для участі в системі.

Алгоритм консенсусу Proof of work є слабким до атаки 51 відсотків, тобто, якщо більше половини вузлів у системі будуть підвласні одній групі зловмисників, то чесні учасники протоколу не зможуть прийти до згоди, і з високою ймовірністю візантійські вузли будуть контролювати ланцюг блоків. Отже кількість чесних вузлів завжди має перевищувати $1/2$ у співвідношенні до усіх вузлів мережі.

1.2 Протокол Casper The Friendly Finality Gadget як надбудова над Proof of Work

Ethereum є другою за величиною криптовалютою у світі за ринковою межею та провідною платформою для децентралізованих програм. Однак нинішня реалізація Ethereum має свої обмеження. Масштабованість для обробки великої кількості транзакцій є однією з головних проблем. Крім того, теперішня залежність Ethereum від алгоритму консенсусу Proof of Work означає, що безпека мережі покладається на мільйони доларів обладнання та величезні затрати електроенергії.

Протокол Casper FFG є гібридним підходом [2]: він зосереджується на багатоступеневому переході до впровадження консунсусу Proof of Stake для мережі Ethereum. У алгоритмі PoS блокчейн додає та погоджує нові блоки через процес, де кожен, хто тримає монети всередині системи, може брати участь, а вплив учаснику протоколу пропорційний впливу кількості монет (або ставки), яку він зберігає. Це набагато ефективніша альтернатива алгоритму доказу роботи (PoW) і дозволяє блокчейну працювати без великих затрат на обладнання та електроенергію.

Casper FFG - це є протокол Proof of Stake, що базується на протоколу стійкості до візантійських помилок (BFT). Відомо за Лампортом, що поки 2/3 учасників чесно дотримуються протоколу, то незалежно від стабільності мережі новий блок може бути доданий до блокчейн. Протокол Casper накладається поверх протоколу генерації блоків і працює незалежно від нього. Casper відповідає за доопрацювання цих блоків, по суті вибираючи унікальний ланцюг, який і буде представляти канонічні транзакції. Casper забезпечує безпеку, але життєздатність залежить від обраного механізму пропозиції. Тобто, якщо зловмисники повністю контролюють механізм пропозиції, Casper захищає від фіналізації двох суперечливі контрольних пунктів, але зловмисники

можуть завадити протоколу фіналізувати будь-які майбутні контрольні точки.

Casper представляє кілька нових функцій, які алгоритми BFT не обов'язково підтримують [3]:

1) Відповідальність. Якщо валідатор порушує правило, можливо виявити порушення та ідентифікувати порушника. Це дозволяє карати зловмисників, вирішуючи питання нульової ставки - проблема, яка зачіпає блокчейн на основі PoS. Штраф за порушення є видалення повного депозиту валідатору. Оскільки надійність Proof of Stake ґрунтується на розмірі штрафу, який може бути встановлений і який може значно перевищувати прибутки від видобутку блоку, це забезпечує суворішу безпеку ніж алгоритм доказу роботи (PoW).

2) Динамічна множина валідаторів.

3) Захист від атаки дальної ревізії та атак, де більше 1/3 від валідаторів виходять в оффлайн.

4) Модульний надшар - Casper полегшує реалізацію протоколу, оскільки його можна використовувати як надбудову над існуючим PoW.

Припускаємо ([3]), що існує фіксований набір валідаторів та механізм пропозиції (наприклад, Proof of Work), який виробляє дочірні блоки існуючих блоків, утворюючи постійно зростаюче дерево блоків. Корінь дерева, як правило, називають «генерующий блок». У випадку порушеної коммунікації через затримки мережі або націлену атаку на блокчейн, обраний механізм пропозиції блоків буде виробляти декількох дітей від одного блоку. Задачею протоколу є обрати єдиний правильний ланцюжок.

Замість того, щоб мати справу з повним деревом із блоків, з метою ефективності Casper розглядає лише підрівень контрольних точок дерева. Кореневий блок є контрольною точкою, а також кожен блок, висота якого в дереві блоків (або його номер) кратне 100 - теж є контрольною точкою. Висота контрольної точки блоку з висотою блоку 100k просто k; еквівалентно, висота $h(c)$ контрольної точки c - кількість елементів у

ланцюгу, що тягнеться від c (не включно) до кореня вздовж батьківських ланок.

Кожен валідатор має власний депозит; коли приєднується новий валідатор, його депозит - це кількість монет на його рахунку. Після приєднання, депозит кожного валідатора збільшується і падає з винагородою та штрафами. Протокол Proof of Stake залежить від розміру депозитів, а не кількість валідаторів, тому коли йде мова про 2/3 валідаторів, мається на увазі кількість учасників, яка зважена за депозитом; тобто набір валідаторів, розмір суми депозиту яких дорівнює 2/3 із загального розміру депозиту усього набору валідаторів.

Валідатори транслюють повідомлення про голосування щодо обраної гілки ланцюгу, що містить чотири відомості [2]: два контрольно-пропускні пункти s та t разом з їх висотами $h(s)$ та $h(t)$. Вимагаємо, щоб s був родоначальником від t на дереві контрольних точок, інакше голосування буде визнано невалідним. Якщо відкритого ключа валідатора v немає в його наборі $<v,s,t,h(s),h(t)>$, голосування теж вважається недійсний.

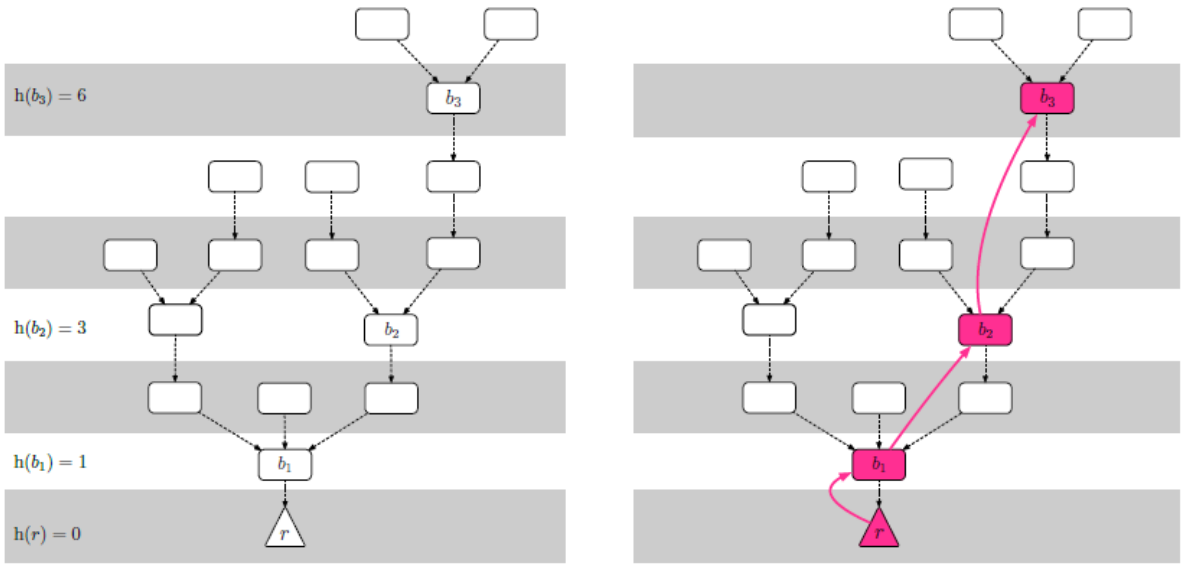

Рисунок 1.1 – Дерево контрольних точок, функція висоти та справедливий ланцюг у мережі

У протоколі виділяють наступні означення [3]:

– Ланцюг за більшістю - це упорядкована пара контрольних точок $(a; b)$, також записана як $a- > b$, така, що принаймні $2/3$ валідаторів (за депозитом) опублікували голоси із джерелом a та цільовим пунктом b. Ланцюг за більшістю може пропускати контрольні точки, тобто, це абсолютно нормально для $h(b) > h(a) + 1$.

– Дві контрольні точки a і b називаються суперечливими, якщо і лише тоді, якщо вони є вузлами в різних гілках, тобто ніхто не є предком, ні нащадком іншого.

– Контрольну точку с називають справедливою, якщо : 1) це корінь або 2) існує ланцюг за більшістю $c'- > c$, в якому контрольна точка c' є також справедливою.

– Контрольна точка c називається завершеною (фіналізуючою), якщо 1) це корінь або 2) вона справедлива і існує ланцюг за більшістю $c- > c'$, де c' - це пряме відгалудження від c. Еквівалентно, контрольна точка c є завершеною тоді і тільки тоді, коли контрольна точка с є справедливою і існує ланцюг за більшістю $c- > c'$, та $'$ не є конфліктними та $h(c') = h(c) + 1$

1.3 Властивості протоколу Casper FFG

Критичні умови протоколу Кожен валідатор не повинен публікувати два різних голоси $<v,s_1,t_1,h(s_1),h(t_1)>$ та $<v,s_2,t_2,h(s_2),h(t_2)>$, такі що :

1. $h(t_1) = h(t_2)$

Тобто, не має публікувати два голоси із однією висотою.

2. $h(s_1) < h(s_2) < h(t_2) < h(t_1)$.

Не має місце публікація голосу у проміжку між іншими.

Найпомітнішою властивістю Casper FFG є те, що неможливо

завершити дві конфліктні контрольні точки, якщо тільки більше ніж $1/3$ валідаторів (за ставкою) порушують одну з двох критичних умов протоколу.

Якщо валідатор порушує будь-яку умову, докази порушення можуть бути включені до блокчейну як транзакція, в цей момент весь депозит валідатора забирається. У нинішньому Ethereum для того, щоб обійти цю умову необхідно провести успішну атаку 51 відсотка.

Ми доводимо дві основні властивості Casper: відповідальність за безпеку та правдоподібну життєдіяльність. Відповідальність за безпеку означає, що два конфліктні контрольні пункти не можуть бути завершені, якщо тільки більше ніж $1/3$ валідаторів (за ставкою) порушують одну з двох критичних умов протоколу. Вірогідна життєдіяльність означає, що незалежно від будь-яких попередніх подій, якщо $2/3$ від усіх валідаторів дотримуються корректної роботи протоколу, тоді завжди можна завершити нову контрольну без порушення критичних умов.

За припущенням, що $< 1/3$ валідаторів за ставкою порушують критичні умови, ми маємо наступні властивості:

(1) Якщо $s_1 - > t_1$ та $s_2 - > t_2$ - два різних ланцюга за більшістю, тоді виконується $h(t_1)! = h(t_2)$.

(2) Якщо $s_1 - > t_1$ та $s_2 - > t_2$ - два різних ланцюга за більшістю, тоді нерівність $h(s_1) < h(s_2) < h(t_2) < h(t_1)$ не має місця.

З цих двух властивостей видно, що для будь-якої висоти n виконується :

(3) Існує якнайбільше один ланцюг за більшістю $s - > t$ з висотою $h(t) = n$.

(4) Існує якнайбільше одна справедлива контрольна точка висоти n.

Теорема 1.1. *Теорема про відповідальність за безпеку : Двоє конфліктующих контрольних точек a_m та b_n не можуть бути обидва завершеними.*

Теорема 1.2. *Теорема про вірогідну життєдіяльність : Ланцюги за більшістю завжди можна додавати для створення нових*

остаточних контрольних пунктів, за умови наявності дітей, що розширюють завершений ланцюг.

Вибір правильного розгалудження. Каспер складніше, ніж стандартні конструкції PoW. Вибір розгалдуження (вилки) повинен бути відрегульований коректно. Модифікований Правила вибору вилки повинні дотримуватися всіма користувачами, валідаторами та навіть механізмом блоку пропозицій, що лежать в основі.

Якщо натомість користувачі, валідатори або блокові пропозиції будуть дотримуватися стандартного правила вибору вилки PoW - «завжди вибирати найдовший ланцюг» є патологічним сценаріїєм, коли протокол «застрягає », а будь-які блоки будуються на вершині найдовшого ланцюга не зможуть бути завершені (або навіть виправданий), без того, щоб деякі валідатори альтруїстично принесли у жертви свої депозити. Щоб цього уникнути, ми вводимо нове, правильне за побудовою, правило вибору вилки: вибирати необхідно той ланцюг, що містить справедливу контрольну точку найбільшої висоти.

Визначення 1.1. Династія блоку є кількість завершених контрольних пунктів починаючи від кореневого до батьківського від даного. Поняття династії необхідно для концепції динамічних валідаторів.

Casper FFG оригінальний документ приводить захист від двух можливих атак проти протоколу. Нас цікавить друга атака – катастрофічні падіння [3].

Припустимо, що більше ніж 1/3 частки валідаторів одночасно виходять з ладу, тобто вони або більше не підключені до мережі, або мають несправності комп'ютера, або самі валідатори введуть себе нечесно. З цього моменту, ніяких данцюгів за більшістю не можна створити, і таким чином ніякі майбутні контрольно пункти не можуть бути доопрацьовані.

Ми можемо відновитись із такої ситуації, встановивши «витік

бездіяльності», який повільно виводить депозит будь-якого валідатора, що не голосує за контрольно пункти, доки з часом розміри його депозитів не зменшаться настільки низько, що валідатори, які голосують, стають більшістю. Найпростіша формула таких витоків – «нехай у кожну епоху валідатору із розміром депозиту D не вдається проголосувати, тоді він втрачає $D * p$ (за $0 < p < 1$), хоча проблема швидкого вирішення проблеми катастрофічних збоїв формулою, яка збільшує швидкість витоку в разі тривалої смуги незавершених блоків.

Цей витечений ефір після цього можна знищити або повернути валідатору через w днів. Чи слід випадені активи спалити чи слід їх повернути, стає поза межами задачі візантійської відмовостійкості і вирішується для конкретних економічних систем по-різному.

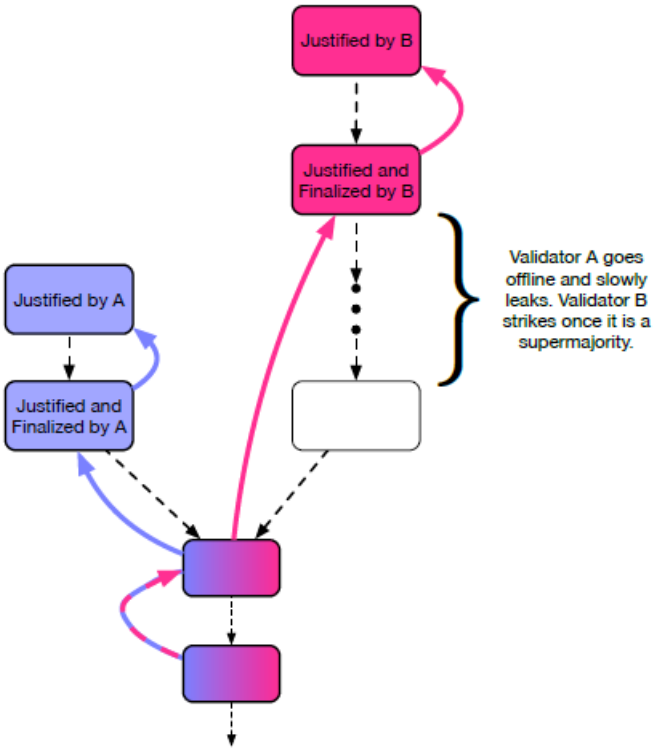

Рисунок 1.2 – Витік ставки через неактивність. Утворення двух завершених точок, що конфліктують.

Витік через неактивність вводить можливість завершення двох конфліктних контрольно-пропускних пунктів без зменшення долі валідатора (рис. 1.2). У такій ситуації валідатори втрачають гроші лише на одному з двох контрольно пунктів. Припускається, що валідатори розбиті на дві підмножини, з підмножиною V_A голосування по ланцюжку A і підмножиною V_B, голосування по ланцюжку B. По ланцюгу A, депозити V_B будуть витікати, і навпаки, що призведе до того, що кожна підмножина має надмірну величину у відповідному протилежному ланцюгу, що дозволяє завершувати дві суперечливі контрольні точки без відсіювання валідаторів (але кожна підмножина втратить значну частину свого депозиту в одному з двох ланцюгів через витоки).

Якщо така ситуація трапиться, то кожен валідатор повинен просто віддавати перевагу тому ланцюгу, де фіналізований пункт пропуску він побачив першим.

Висновки до розділу 1

У розділі розглянуто протокол валідації блокчейну для криптосистеми Ethereum – Casper the Friendly Finality Gadget. Протокол використовується як надбудова над існуючим адгоритмом генерації блоків, наприклад, Proof of Work і не заважає його роботі. Головна мета протоколу – набір із валідаторів має обрати єдину гілку у дереві блоків, використовуючи гібрид між алгоритмами PBFT та Proof of Stake.

2 ДОСЛІДЖЕННЯ НАДІЙНОСТІ ПРОТОКОЛІВ, ПОБУДОВАНИХ НА ТЕХНОЛОГІЇ БЛОКЧЕЙН.

У цьому розділі розглядається вплив властивостей CAP теореми на технологію блокчейн, їх співвідношення між собою. Пропонується модель надійності на етапі експлуатації для протоколу консенсуса Casper FFG і ідеї для подальшого її дослідження.

2.1 Модель надійності для протоколу Casper FFG

Технологія блокчейн функціонує за рахунок алгоритму консенсусу, який відповідає за те, щоб усі вузли в мережі блокчейн прийшли до узгодження. Формально, це означає, що алгоритм має вирішувати задачу Візантійських генералів, тобто приймати рішення, незважаючи на наявність m візантійських вузлів.

Для дослідження надійності алгоритмів консенсусу моделюємо децентралізовану розподілену систему : розглянемо ситуацію, коли усі учасники мережі є чесними у сенсі коректної роботи програмного забезпечення, роботи мережі, тощо. При цьому допускається візантійська поведінка учасника : він може свідомо порушувати довірчу середу, намагаючись обманути протокол. При таких умовах алгоритми мають свої співвідношення на кількість нечесних вузлів, до яких вони є «терплячими» ($<1/2$ від усіх для PoW, $<1/3$ - для PBFT).

Реальні системи однак, мають враховувати ненавмисні помилки учасників мережі, ситуації, коли відбувається «падіння» вузла або некоректність комунікаційних каналів, інше. В таких випадках логічно, що цілеспрямованій группі зловмисників не потрібно буде досягати граничного співвідношення, оскільки в силу випадкових помилок

учасників, значення цього співвідношення буде падати.

Основним випадком некоректної роботи мережі у даному дослідженні розглядається поведінка візантійського характеру при умові, що власне мережа працює безпомилково. Однак для подальшого дослідження слід розглянути ситуацію, коли повідомлення не передаються через комунікаційні канали без помилок. Хоча шумні канали з нульовою ємністю помилок існують, більший практичний інтерес представляє ситуація протилежна. Помилки при передачі є неминучими, це стосується наявності у будь-якому каналі зв'язку шуму, який є загальною сумою усіх випадкових сигналів. Для того, щоб взяти такі помилки передачі до уваги, необхідне деякі виправлення в схемах кодування, наприклад, розглянемо просту модель передачі даних при наявності шуму - бінарний симетричний канал. Такий канал розрізняє лише два символи, що як правило, інтерпретуються як 0 і 1; при цьому симетричний означає, що помилки однаково ймовірні незалежно від переданого символу.

Нехай ймовірність безпомилкової передачі буде позначена як p, а зашумленої відповідно $1 - p$. В такій моделі для спрощення вважаємо, що комунікаційний канал не підтримує затримок у часі. Для Pow консенсусу це означає, що ймовірність попасти у ланцюг більшості учасників протоколу збільшується для того, хто вирішив задачу першим.

Тому час буде розглядатися як основний параметр для надійності у такій моделі. Ми кажемо, що блокчейн не є надійним, коли час для узгодження нового блоку перевищує деякий відомий поріг , тим самим це суперечить здатності системи виконувати задані функції за умови втручання (помилки, збої, падіння нод). Ситуація, коли часовий ліміт перевищується лише за рахунок не здатності мережі генерувати новий блок для деякого часу $t > T_{limit}$ є дуже малоймовірною, щоб її розглядати, оскільки мережа PoW час від часу змінює складність вирішення проблеми спеціально так, щоб блок можна було знайти у відповідному часовому інтервалі.

Для практичного інтересу розглянемо ситуацію для консенсусу PoW, коли блок B не може бути узгоджений більшістю вузлів, тобто, більше половини учасників протоколу не містять блоку B у своїх ланцюгах і кожні блоків, необхідних для валідації, які йдуть після цього, теж не можуть бути узгоджена більшістю.

Ми припускаємо, що блок B, породжений деяким майнером, не буде включений до іншого вузла блокчейна якщо: 1) цей вузол - візантійський; 2) цей вузол випав оффлайн через збої програмного забезпечення; 3) майнер, який вирішив складну задачу не зміг передати знайдений блок до цього вузла через некоректний канал зв'язку. Загальна кількість таких вузлів повинна бути більшою ніж половина всіх учасників протоколу для всіх блоків валідації поспіль, так, щоб перший з них не був узгодженим за час валідації, встановлений мережею.

Таким чином, припущення щодо помилкових каналів комунікації призвели до незручних для дослідження і малоймовірних ситуацій повної ненадійності системи. В подальшому вважаємо, що мережа може прийти до ненадійності лише за рахунок візантійських помилок вузлів, вважаємо, що вузли працюють коректно, але не захищені від помилок їх ПЗ.

За [4] при побудові моделі помилок у ПЗ робляться наступні припущення:

- інтервали часу між спотвореннями, що виявили, є статистично незалежними.

- інтенсивність прояву помилок залишається сталою, доки не проводиться їх виправлення, однак частота виявлення помилок та частота їх виправлення не рівні, але зв'язані деяким коефіцієнтом пропорційності; якщо усувати кожну знайдену помилку, інтервали часу між їх проявами змінюються за експоненційним законом.

- в процесі тестування можуть виявлятися та накопичуватися групи помилок, які утворюють чергу для корекції програми; припускається, що довжина черги виявлених та чекающих на виправлення помилок визначається пуассонівським потоком, вибір помилок з усіх проводиться

випадково, а витрати праці на корекцію помилок порядкуються експоненційному закону розподілу.

Нехай, в якості моделі розподіленої системи розглядаємо систему масового обслуговування з відказами. Заявками в розумінні моделі виявлення спотворень у ПК вважаємо помилки, які під час експлуатації системи проявляються у деяких вузлах (каналах). Тобто, завяка, що прийшла до каналу інтерпретується, як виявлення помилки на вузлі.

Адекватність такої моделі базується допущеннях про показниковий розподіл часу обслуговування (допускаємо в рамках моделі) та пуассоновський характер потока заявок, що означає виконання двох властивостей: процес у системі має бути стаціонарним та майбутні зміни мають не залежати від змін у минулому.

Очевидно, що на початку, відразу після включення системи в роботу, процесс, що відбувається, не буде стаціонарним, в системі масового обслуговування (як і в будь якій динамічній системі) виникне так званий «перехідний», нестаціонарний процес. Однак, після деякого часу, цей перехідний процес затухне, і система перейде на стаціонарний, так званий «установлений» режим, ймовірнісні характеристики якого вже не будуть залежати від часу.

Нехай, маємо n - канальну систему масового обслуговування з відказами, тобто в термінах децентралізованого протоколу - n учасників мережі. Розглянемо її як фізичну систему X із скінченою множиною станів:

x_k - зайнято рівно k каналів (помилкова робота к вузлів у мережі)

k = 0,...,n

Маємо визначити ймовірності станів системи p_k (k=0,1,...,n) для будь-якого моменту часу t. Задачу вирішуємо при наступних допущеннях [5]:

1) Маємо потік заявок з щільністю λ

2) час обслуговування (звільнення канала від заявки, тобто усунення помилки) має показниковий розподіл із параметром $\mu = \frac{1}{m_t}$

З такими допущеннями маємо марковский випадковий процес і

використовуючи його апарат можемо отримати [5]:

$$g(t) = \mu e^{-\mu t}$$

Параметр μ аналогічен до параметра λ показникового закону розподілу проміжку T між сусідніми подіями простішого потоку:

$$f(t) = \lambda e^{-\lambda t}$$

λ має сенс щільності потоку заявок(помилок), і аналогічно величину μ можна розглядати як «щільність потоку звільнень». Визначимо ймовірності $p_0(t)$, $p_1(t)$,..., $p_n(t)$ прийняти можливі стани системи x_0,x_1, ..., x_n. Для будь якого моменту часу виконується

$$\sum_{k=0}^{n} p_k(t) = 1$$

Використовуючи апарат теорії ймовірностей, обраховуємо ймовірності переходу системи з одного стану в інший. Приходимо до диференціального рівняння для $p_0(t)$:

$$\frac{dp_0(t)}{dt} = -\lambda p_0(t) + \mu p_1(t)$$

Аналогічні диференційні рівняння будуються і для інших ймовірностей переходу станів.

$$\frac{dp_k(t)}{dt} = p_{k-1}(t)\lambda - (\lambda + k\mu)p_k + \mu(k+1)p_{k+1}(t)$$

Отже, загальна система диференційних рівнянь виглядає наступним чином:

$$\begin{cases} \frac{dp_0(t)}{dt} = -\lambda p_0(t) + \mu p_1(t) \\ \ldots\ldots\ldots\ldots \\ \frac{dp_k(t)}{dt} = p_{k-1}(t)\lambda - (\lambda + k\mu)p_k + \mu(k+1)p_{k+1}(t) \\ \ldots\ldots\ldots\ldots \\ \frac{dp_n(t)}{dt} = \lambda p_{n-1}(t) - n\mu)p_n \end{cases} \tag{2.1}$$

Оскільки цікавлять граничні величини, система переводится у свій алгебраїчний аналог шляххом заміни всіх ймовірностей на граничні.

$$\begin{cases} -\lambda p_0 + \mu p_1 = 0 \\ \lambda p_0 - (\lambda + \mu)p_1 + 2\mu p_2 = 0 \\ \ldots\ldots\ldots\ldots \\ \lambda p_{k-1} - (\lambda + k\mu)p_k + (k+1)\mu p_{k+1} = 0 \\ \ldots\ldots\ldots\ldots \\ \lambda p_{n-2} - (\lambda + (n-1)\mu)p_{n-1} + n\mu p_n = 0 \\ \lambda p_{n-1} - n\mu)p_n = 0 \end{cases} \tag{2.2}$$

Вирішуючи нову систему 2.2 відносно невідомих ймовірностей, отримаємо величину, що цікавить:

$$p_k = \frac{\lambda^k}{k!\mu^k} p_0 \tag{2.3}$$

для будь-якого $k <= n$

Величина $\alpha = \frac{\lambda}{\mu}$ є приведена щільність потоку заявок, тобто середня кількість заявок, що приходять на середній час обслуговування однієї заявки. В рамках розглянутої моделі виникнення помилок ця величина

означає середню кількість помилок, що виникає за середній час, необхідний для виправлення одного спотворення.

Тоді $\alpha = \lambda m_t$, де m_t - середній час обслуговування однієї заявки. У нових позначеннях формула (2.3) приймає вигляд

$$p_k = \frac{\alpha^k}{k!} p_0 \tag{2.4}$$

$$p_k = \frac{\frac{\alpha^k}{k!}}{\sum\limits_{i=0}^{n} \frac{\alpha^i}{i!}}$$

Таким чином, отримавши ймовірності $p_0(t)$,$p_1(t)$, ... , $p_n(t)$, можна знайти середню кількість нечесних вузлів серед усіх учасників децентралізованого протоколу, тобто в них була виявлена помилка, що призвело до збою в роботі.

Нехай ξ - випадкова величина, що приймає значення 0,1,2,...,n. Кожне можливе значення k означає, що в системі має місце стан x_k із ймовірністю p_k (працюють із збоями k вузлів). Тоді математичне сподівання випадкової величини ξ є середня кількість нечесних вузлів.

$$M\xi = \sum_{k=0}^{n} k p_k$$

Протокол Casper FFG є Proof of Stake орієнтованою системою, що базується на PBFT. Тому, необхідно враховувати, що падіння деякого вузла мережі не є еквівалентно зменшенню показників співвідношення чесних і нечесних учасників на деяку логічну одиницю, оскільки у PoS-орієнтованій системі мають значення не самі валідатори, а ставки, які вони роблять.

Таким чином, приходимо до наступної величини, що характеризує надійність системи (на етапі експлуатації):

$$\sum_{k=0}^{M\xi} s_k \leq \frac{1}{3} \sum_{k=0}^{n} s_k$$

де s_i - величина ставки i-ого валідатора. Ця величина означає

кількість депозиту від суми ставок кожного валідатора у блокчейні, що є візантійським вузлом. Для досягнення стану ненадійності системи необхідно, щоб порушувалась умова протоколу PBFT, тобто, вказана сума перевищувала третину від суми усіх ставок усіх валідаторів.

Для подальшого аналізу можемо використати формальний фреймворк для блокчейнів, що використовують консенсус Proof of Stake [6], а саме:

$(\beta,\ l)$ – достатній вклад ставки: сукупний розмір ставки, представленої чесними учасниками блокчейну в будь-якій послідовності із l або більше послідовних блоків є не меншою за β долі від загальної ставки в системі блокчейну із незначною ймовірністю;

$(\gamma,\ l)$ – достатній чесний вклад ставки: сукупний розмір чесно утриманої ставки, представленої чесними учасниками блокчейну в будь-якій послідовності із l або більше послідовних блоків є не меншою за β долі від загальної ставки в системі блокчейну із незначною ймовірністю;;

Вважаємо, що ці властивості з відповідними параметрами вже отримані (розглядаємо як чорний ящик), для припущення щодо певного розподілу ставок між чесними вузлами. Тоді можна оцінити надійність блокчейну, використовуючи дані параметри для l рівного одному блоку, наступним чином:

$$n(\beta - \gamma) \leq \sum_{k=0}^{M\xi} s_k$$

Необхідно зазначити, що при аналізі параметрів PoS блокчейна ми робимо певні спрощення припущень щодо моделі. По-перше, ми вимагаємо, щоб кількість чесних майнерів, які активно беруть участь у прийнятті рішень (тобто знаходяться онлайн), а також сума ставки, яку вони спільно утримують, не опускалася нижче певного порогового значення. Тобто, очікуємо, що (чесні) валідатори, які контролюють значну кількість ставок, не залишаться оффлайн протягом достатньо

довгих періодів. Однак не вважається, що всі чесні вузли є активними, як і не вважається, що всі чесні групи, що мають більшу частку ставки залишаються онлайн. Ми вимагаємо лише, щоб кількість таких чесних учасників не опускалася нижче деякого ліміту.

2.2 CAP теорема у розумінні блокчейна

Теорема CAP — гіпотеза, що для будь-якої розподіленої комп'ютерної системи неможливо одночасно забезпечити виконання більше двох із перелічених трьох властивостей:

1) узгодженість даних (C) (усі вузли бачать однакові дані у будь-який момент часу або запит на читання дає останні актуальні дані);

2) доступність (A) (гарантія того, що кожен запит отримає відповідь без помилок, незважаючи на те, читає клієнт останні записанні дані чи ні);

3) стійкість до розділення (P) (попри розділення на ізольовані частини або втрати зв'язку з частиною вузлів, система не втрачає стабільність і здатність коректно відповідати на запити).

У системах типу Інтернет не можна повністю гарантувати властивість P, обмежуючи вибір доступністю та узгодженістю даних. Оскільки доступність грає найбільшу роль для комерційних мереж, задача розробки системи розподілених баз даних для підприємства зводиться до задачі вибору між різними можливими стратегіями відновлення властивості узгодженості [7].

У блокчейні ймовірність, що система розділиться на підчастини, є значно більше ніж виникнення такої ситуації для традиційної бази даних, оскільки блокчейн фактично моделює випадок, що виникає в системах баз даних, де сторони, які є повністю недовіреними або лише частково довірені, беруть мають у мережі рівны умови.

Можливі не лише випадкові поділи системи через збої в мережі або власне на вузлах, але і в ситуації, коли публічний блокчейн повинен мати справу зі зловмисно створеними розгалудженнями, вилками у ланцюгу за рахунок змагання вузлів щодо генерації блока, поділом через неможливість учасників протоколу прийти до загального рішення [7].

Для блокчейну важливим питанням є дослідження надійності, узгодженості та стійкості до розділення на підсистеми із врахуванням

CAP теореми. Як правило, усі розподілені системи жертвують властивістю «доступності» (A) або узгодженості (C) на користь властивості «стійкості до розділення на підсистеми» (P), тобто маємо справу або із AP системами або із CP системами.

Для того, щоб бути AP, клієнт повинен приймати транзакцію, як тільки він додається до блокчейну. Таким чином, що немає залежності від решти вузлів, щоб зробити її валідною, але існує ризик того, що решта учасників відхилять транзакцію, втрачаючи узгодженість системи. Для того, щоб бути CP мережею, клієнт повинен прийняти транзакцію лише після того, як блокчейн прийщов до консенсусу щодо неї. Таким чином, зберігається узгодженість, але система ризикує стати недоступною, якщо є розгалудження, що заважають утворити консенсус між вузлами.

Якщо обрати доступність над узгодженністю в блокчейні, то будь-які запити на читання не гарантовано будуть отримувати актуальні дані на той момент часу. Незважаючи на те, що в такому випадку мережа завжди дає відповідь, задача блокчейна як довірчого посередника зникає. Однак, відсутність властивості узгодженості - не є приємлемим в жодній комерційній системі. Узгодженість завжди має пріоритет у технології блокчейн. Однак при зневажанні властивістю доступності як необов'язковою функцією, бачимо, що це змушує мережу бути недоступною при наявності розгалудження, що приводить до порушення консенсусу. Отже, доступність не може бути знехтувана в технології блокчейн, оскільки алгоритм консенсуса є ключовим.

Окремою проблемою, специфічною для криптовалют типу біткоіну є проблема виявлення факту стійкості до поділу системи на частини (наприклад, DOS-атаки на блокчейни – саме той випадок, коли «P властивість» порушується).

Для виявлення «властивості P» в повністю децентралізованій розподіленій системі, якою і є блокчейн, потрібен специфічний алгоритм консенсусу, тобто спосіб учасників проголосувати за справжній стан даних за наявності розгалуджених ланцюгів. Для візантійських

протоколів узгодження Paxos і Raft ця задача вирішується достатньо просто. У цих системах запис вважається виконаним, якщо більшість вузлів у мережі приймає його. Але в протоколах PoW або PoS кількість активних вузлів (майнерів) постійно змінюється, тому визначення «більшості» є проблематичним. Можливо показати, що в загальному випадку, для PoW(PoS) блокчейнів проблема виявлення P є невирішуємою та досягнення C (тобто мережа PC) є неможливим.

Розглянемо ситуацію, коли деяка кількість майнерів блокчейна в результаті розділення мережі стають відірваними від глобального ланцюга, але продовжують утворювати блоки та валідувати транзакції між собою. В такому випадку для цієї групи майнерів немає різниці, продовжує роботу глобальний блокчейн чи ні, однак якщо вони згодом налагодять синхронізацію із зовнішнім пулом валідаторів, то пам'ять їх менш потужного блокчейна буде стерта більш потужним. Однак, в силу того розмір мережі може змінюватися, для них не існувало надійного способу визначити, чи присутня більшість учасників. Ось чому біткоін не може забезпечити узгодженість і система PC є недосяжною.

Зазвичай у блокчейні вибирають оптимальний варіант AP-системи та, залежно від задач та цілей блокчейну, властивість узгодженності. Наприклад, для біткоіну, що використовує алгоритм консенсусу Proof of Work, «степінь» узгодженості виражається в кількості блоків в ланцюгу, необхідних для валідації першого з них, тобто 6.

З цього приводу постає питання про час очікування на надійну (валідну) транзакцію і звідси питання про потенційне принципове обмеження швидкості блокчейнів із різними алгоритмами консенсусу, відмінними від візантійських.

Для блокчейнів із PoW консенсусом у випадку маштабного розділення ланцюга час очікування валідної транзакції збільшується із зменшенням обчислювальної потужності/кількості майнерів, що відповідно призводить до уповільнення мережі. Для PoS орієнтованної системи може ймовірніше виникнути проблема централізації, однак

швидкість блокчейну не має зазнати змін.

Протокол Casper FFG проте, може стати оптимальним рішенням для цих алгоритмів консенсуса, так як він фактично надбудовою над будь-яким алгоритмом генерації блоків. У ситуації відділення групи майнерів від головної мережі, валідатори Casper зможуть помітити їх відсутність — Casper має динамічний пул валідаторів і для виходу із цього пулу необхідно включити в блок династії d «withdraw»-повідомлення, щоб вийти на династії $d + 2$. У випадку наявності неактивних валідаторів, що знаходяться у оффлайн режимі (падіння вузлів) і не роблять ставок протокол вводить поняття «витоку через неактивність». Поступове зменшення депозиту у неголосующих за чекпоінти валідаторів дає змогу проводити голосування іншим, а саме — зв'язок за більшістю (елемент візантійського протоколу).

Протокол Casper за рахунок використання елементів візантійського узгодження (алгоритму BFT) не приходить до проблеми зменшення швидкості блокчейну. При виникненні ситуації відділення декої частини пула валідаторів та згодом формування ними чекпоінтів між собою, поєднання двох суперечливих ланцюгів відбувається за візантійською більшістю — обирають ту пару чекпоінтів, що утворюють зв'язок за більшістю.

Висновки до розділу 2

В цьому розділі було досліджено протокол Casper the Friendly Finality Gadget на надійність на етапі експлуатації — показали, як можна оцінити кількість нечесних валідаторів у сенсі ненадійності їх програмного забезпечення. Було розглянуто концепцію протоколів Casper FFG, PoW як AP і CP систем, окремою проблемою виділено нездатність блокчейну вирішувати ситуацію розділення ланцюга на незалежні частини.

3 ХАРАКТЕРИСТИКИ БЛОКЧЕЙНІВ BITCOIN І ETHEREUM

3.1 Проблема масштабуємості блокчейнів та її вирішення

Поставлені у минулому розділі питання щодо залежності швидкості блокчейну і очікування валідної транзакції можно спостерігати у різних розподілених блокчейн-системах. Такі блокчейн мережі, як Bitcoin і Ethereum, мають суттєве обмеження, що уповільнює їх реалізацію, проблему масштабованості: критичне зниження пропускної здатності і швидкості транзакцій при істотному зростанні обсягів транзакцій.

Проблема масштабованості виникла через те, що розробникам блокчейнів довелося вирішувати так звану трілему блокчейна, коли із трьох якостей: децентралізація, безпека і масштабованість, необхідно віддати перевагу двом. Децентралізація означає, що кожен вузел має доступ до певної кількості ресурсів системи, що дає їй змогу коректно працювати, ця властивість відповідає доступності. Безпека означає стійкість до розділення, стійкість до проведення атак на систему із визначеною кількістю ресурсів. Масштабованість говорить пор кількість транзакцій, які може обробити система.

Розробники платформ Bitcoin і Ethereum серед цих властивостей обирають безпеку і децентралізацію, тому їх системи не є масштабуємі. Іншим прикладом є відмова приватних блокчейнов (Hyperledger, Corda, Quorum) від децентралізації на користь збільшення швидкості. Щоб не йти на компроміси і отримати всі три якості, потрібно заново винайти спосіб побудови децентралізованої мережі. Для біткоіну головні претенденти на вирішення проблеми масштабованості є технології Lightning Network і RootStock. Для Ethereum перспективними є технології Sharding, Plasma і Casper.

Lightning Network

Lightning Network — це є надбудова над основним механізмом

пропозиції блоків, в основі якої лежить ідея, що не всім учасникам мережі потрібно тримати всю історію транзакцій для підтримки ефективної синхронізації мережі. Ця ідея є основою підходу з використанням спрямованого ациклічного графа (DAG). Блокчейн заснований на «вертикальної архітектурі», тоді як DAG працює за «горизонтальною» схемою. У блокчейні транзакції групуються у нові блоки, які потім додаються в ланцюжок блокчейна. У «горизонтальній» схемі мережи DAG транзакції безпосередньо зв'язуються з іншими транзакціями, що відбулись раніше, групуючи їх в блоки. У випадку мереж, де нові транзакції підтвержують старі, старий платіж ніколи не перевірить новий, тобто, перевірка завжди йде вперед і ніколи не утворює циклу [8].

Оскільки структура DAG схожа на верифікації, її досить часто називають клубком (tangle), що має аналогічні властивостями, що і децентралізований блокчейн: розподільний реєстр, заснований на тимчасовій мережі. Отже, Tangle, як і блокчейн, є механізмом валідації розподіленого прийняття рішень. Цей клубок (криптовалюта IOTA) створюється шляхом зв'язування окремих транзакцій в єдину тимчасову мережу. Зв'язки між транзакціями формуються на базі простого правила: щоб нова транзакція була підтверджена, вона повинна підтвердити дві старші транзакції, кожна з яких підтвердила всі інші ще більш старіші транзакції.

На відміну від блокчейна біткоіна або Ethereum, де транзакції валідують майнери в обмін на винагороду, у Tangle функція обробки і затвердження платежів покладена на усіх активних учасників мережі. Кожен користувач, охочий провести транзакцію, підтверджує дві інші нові транзакції і побічно валідує всю історію транзакцій. Таким чином, мережа Tangle врятована від необхідності платити майнерам за внесення транзакцій до блоку, внаслідок чого в мережі немає транзакційних комісій. І оскільки немає необхідності створювати блоки, то транзакції підтверджуються дуже швидко: чим більше активних учасників, тим більше пропускна здатність мережі. Таким чином, на відміну від

блокчейну, системи, що використовують tangle здатні до маштабування і швидкість мережі зростає із збільшенням кількості активних учасників у мережі.

Rootstock

RSK є ще одною надбудовою над біткоіном, яка дозволяє будувати смарт-контракти і підключена до блокчейн-ланцюга за допомогою технології побічних ланцюгів (Sidechain) [9].

По своїй суті, Rootstock є поєднанням наступних елементів:

- Детермінована машина Тьюрінга - Двосторонній побічний біткойн-ланцюг (для обміну номіналом BTC) - Динамічний гібридний протокол консенсусу майнінгу та мережа з низькою затримкою (для швидких платежів).

Блокчейн RSK захищений технологією "злиття майнінгу що означає, що він буде настільки стійким як і біткойн, коли мова йде про захист атаці подвійних витрат. RSK має потенціал для збільшення масштабів біткоіна далеко за межі його поточного стану. RSK може масштабувати до 300 транзакцій в секунду, і для цього не має потреби жертвувати децентралізацією та зменшувати місце для зберігання.

Шардінг

Шардінг — це спосіб масштабувати блокчейн Ethereum, використовуючи роботу автономних блокчейнов (шардів) зі своїми локальними реєстрами. Це дозволить збільшити пропускну здатність мережі, що важливо в разі Ethereum, який в ідеалі має бути інфраструктурою для децентралізованих додатків[10].

Валідатори будуть відповідати за підтвердження транзакцій в шардах. Щоб стати валідатором, потрібно буде витратити на це не менше 32 ефірів (близько 10 тисяч доларів за даним курсом). Згідно з останньою версією Ethereum, мінімально рекомендується використовувати 111 валідаторів для однієї шарди, об'єднаних в «комітет».

Валідатори так само як і майнери отримуватимуть нові монети в нагороду за валідацію блоків. Чим більше загальне число монет у

валідаторів в мережі, тим більше емісія монет. З технічної точки зору стати валідатором набагато простіше, ніж майнером, і в Ethereum сподіваються, що це стане масовим заняттям, хоча виникають сумніви щодо прибутковості. Проте швидше за все встановиться баланс - валідатори будуть регулювати обсяг ставки в залежності від ціни ефіру: знижувати його при зниженні вартості активу, і навпаки.

Одні з основних проблеи шардінга є наступні: захоплення одного шарда — атакуючий захоплює більшість валідаторів на одному шарду, або перешкоджає отриманню достатньої кількості підписів, або, відправляє недійсні підписи; State transition execution - атака на один шард, зазвичай запобігання якої є за допомогою випадкової вибірки, але такі схеми ускладнюють отримання даних про стан шарду, так як вони не можуть мати оновлену інформацію кожного вузла, якому можуть бути призначені. Не можливо точно гарантувати те, що "легкі вузли все ще можуть отримати точну інформацію про стан шарда.

Plasma Ethereum

Основна ідея Plasma-технології полягає у створенні фреймворка побічних ланцюгів, які будуть якомога рідше взаємодіяти з основним блокчейном. Такий фреймворк призначений для роботи у вигляді блокчейн дерева, яке ієрархічно організовано таким чином, що безліч дрібних ланцюжків (плазма ланцюги) може бути створено поверх основного [11].

Структура Плазми пов'язана з використанням смарт-контрактів і дерев Меркле, що дозволяє створювати необмежену кількість малих ланцюжків, які по суті є меншими копіями основного Ефіріум блокчейна. У кожного малого ланцюга так само створюється велика кількість інших ланцюжків, що порождає деревоподібну структуру.

По суті, кожна малий плазма ланцюг являє собою гнучкий смарт-контракт, який може бути розроблений так, щоб працювати єдиним чином, відповідаючи різним потребам. Це означає, що ланцюги можуть співіснувати і працювати незалежно. Зрештою, Plasma дозволяє

запроваджувати масштабовані рішення різними способами відповідно до їх конкретних потреб.

Впровадження Plasma зменшує ймовірність того, що головний ланцюг буде перевантажений, оскільки кожний малий ланцюг буде розроблений для роботи певним чином, для досягнення своїх конкретних цілей, які не обов'язково пов'язані с основний ланцюжком. Таким чином малі ланцюги полегшують загальну роботу основного блокчейна.

Однією з основних проблем пов'язаних з Плазмою, є проблема масового виходу, яка відноситься до сценарію, в якому багато користувачів намагаються одночасно вийти зі свого Plasma ланцюга, заповнюючи кореневий ланцюг і викликаючи перевантаження великої мережі. Це може бути викликано шахрайської діяльністю, мережевими атаками або будь-яким іншим видом критичного збою, який може мати малий Plasma ланцюг або група ланцюжків.

Висновки до розділу 3

У цьому розділі запропонували і розглянули можливі вирішення проблеми масштабуємості для блокчейнів типу Ethereum та Bitcion. Ця задача тісно пов'язана із обмеженням на швидкість та кількість оброблених транзакцій у блокчейні. Для біткоіну головні претенденти на вирішення — це технології Lightning Network і RootStock. Для Ethereum перспективними є технології Sharding, Plasma і Casper.

ВИСНОВКИ

У ході даної роботи був проведений аналіз опублікованих джерел, розглянуто протокол консенсусу Casper the Friendly Finality Gadget як надбудову над блокчейном системи Ethereum. Протокол являє собою своєрідне поєднання двох алгоритмів узгодження: Proof of Stake та візантійський PBFT.

Протокол був досліджений на надійність на етапі експлуатації з метою отримати її оцінки — розглянули надійність розподілених систем як вирішення протоколом задачі Візантійських генералів, тобто, оцінили співвідношення кількості «чесних» (коректно працюючих) вузлів до числа несправних (у сенсі ненадійності їх програмного забезпечення) вузлів мережі, при якому система працює коректно. Отримали можливість оцінювати величину, що характеризує надійність, тобто середню кількість нечесних вузлів: з одного боку нерівності вона обмежена границею візантійського консенсусу (PBFT), з іншої сталими величинами, що описують властивості розглядаємого PoS-блокчейна, а саме — достатній вклад ставки та достатній чесний вклад ставки.

У роботі було розглянуто застосування CAP теореми до блокчейна, концепцію протоколів Casper FFG, PoW як AP і CP систем, побачили; що оптимальним варіантом для блокчейну є AP-системи з деякою варіацією властивості узгодженості. Було досліджено, як алгоритм Proof of Work, Proof of Stake та консенсус Casper FFG зіткаються із проблемою CAP гіпотези — нездатність блокчейну виділити ситуацію розділення ланцюга на незалежні частини, що призводить до порушення швидкості блокчейну.

Проблема порушення швидкості валідації транзакцій може бути і наслідком проблеми масштабуємості для публічних блокчейнів. Було розглянуто, які технології та протоколи можуть стати вирішенням цієї задачі для біткоіна та етеріуму. Для біткоіну — це технології Lightning

Network і RootStock. Для Ethereum перспективними є Sharding, Plasma і Casper.

ПЕРЕЛІК ПОСИЛАНЬ

1. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction / Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder, Princeton University Press, July 19, 2016. 336 с.

2. Ethereum Casper: A Comprehensive Guide [Електронний ресурс] – Режим доступу до ресурсу: https://www.skalex.io/ethereum-casper/

3. Buterin V. Casper the Friendly Finality Gadget / V. Buterin, V. Griffith., 2017. – 10 с.

4. В.В. Липаев Надежность и функциональная безопасность комплексов программ реального времени. - М.: 2013. . - 176 с.

5. Математическое моделирование систем связи : учебное пособие / К. К. Васильев, М. Н. Служивый. – Ульяновск : УлГТУ, 2008. – 170 с.

6. Rishab G. Overcoming Cryptographic Impossibility Results using Blockchains / Rishab Goyal, 2017. – 48 с.

7. Keir Finlow-Bates CAP Is Not the Whole Story: Introducing Trust and Blockchain [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://dzone.com/articles/adding-trust-to-cap-blockchain-as-a-strong-eventua

8. Lightning Network [Електронний ресурс] – Режим доступу до ресурсу: https://lightning.network.

9. The Ultimate Guide to Rootstock Blockchain [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://blockgeeks.com/guides/rootstock-blockchain/

10. Путь к Ethereum 2.0. Часть 2: шардинг, eWasm и новая экономика [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://media.unitedtraders.com/posts/22541-put-k-ethereum-20-chast-2-sharding-ewasm-i-novaya-ekonomika

11. Ethereum Plasma [Електронний ресурс] – Режим доступу до ресурсу: https://www.binance.vision/ru/blockchain/

what-is-ethereum-plasma.

12. Castro M. Practical Byzantine Fault Tolerance / M. Castro, B. Liskov // Proceedings of the Third Symposium on Operating Systems Design and Implementation. – 1999.

13. 20. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System / Satoshi Nakamoto., 2009. – 9 с.

14. Juin Chiu Casper FFG: Consensus Protocol for the Realization of Proof-of-Stake [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://medium.com/unitychain/intro-to-casper-ffg-9ed944d98b2d